

## REMARKS

*Claim rejections – 35 USC §112*

Claims 3 - 4 have been amended to make it clear, as suggested by the examiner, that the “pre-printed serial number” is printed on the blank test certificate. Claim 5 has been rewritten in independent form as new claim 20, including similar amendments. It is believed that these amendments overcome the rejection in paragraphs 4 - 5 of the detailed action.

Regarding the rejection of claim 16 in paragraph 6 of the detailed action, it is respectfully submitted that it is not appropriate to include references to printing the test certificate only if the test receives a passing mark. It is submitted that it would be appreciated by one skilled in the art that in some cases a test certificate might be required to show the result of a test, even if the result is “failure” (and indeed the concept of “failure” might not be relevant to some tests). It should be noted that the words used in the claim are “test certificate”, not “pass certificate”. Although in the described embodiment of the invention different blank forms are used for pass and failure, it is submitted that it would be clear to one skilled in the art that the same form could easily be used for both pass and failure; in this case, the results of the test printed on the form could themselves indicate whether the test had been passed or failed (e.g. simply by printing the word “Passed” or “Failed” on the certificate). In other cases, a test may simply give a result, without any classification as pass or failure.

*Claim rejections – 35 USC §103*

Claims 2-4, 6-11 and 16 were rejected as unpatentable over Walker et al. (U.S. Patent No. 5,828,751) in view of Schneier (Applied Cryptography, 2nd Edition). Reconsideration is urged.

Walker describes a method for secure measurement certification, in which a measurement is made by a sensor 8 and augmented by the time from a clock. A cryptoprocessor 10 then creates a certified measurement, comprising the cleartext augmented measurement and a ciphertext one-way function (e.g. a hash) of the augmented measurement (column 8, lines 2-11). Instead of hashing, encryption can be used (column 9, lines 3-7). The certified measurement is fed to an output device 100, which may be a printer for recording the certified measurement on to a piece of paper (column 10, lines 26-29). In the case where hashing is used, the recipient of the certified measurement reads the cleartext part and recomputes the hash to verify the ciphertext.

part (column 11, lines 7-12). Where encryption is used, the recipient verifies the measurement by decrypting the encrypted measurement (column 11, lines 13-16).

Schneier (page 35) describes the use of a trusted third party (arbitrator) to provide digital signing of documents. The parties to the protocol are referred to as Alice and Bob, and the trusted third party as Trent. Alice encrypts her message using a secret key  $K_A$  shared by Alice and Trent, and sends it to Trent. Trent decrypts the message using  $K_A$ , and re-encrypts it, along with a statement that he received this message from Alice, using a secret key  $K_B$  shared by Trent and Bob, and sends it to Bob. Bob decrypts the message using  $K_B$ . Because Bob trusts Trent, Bob knows that the document really came from Alice.

It is respectfully submitted that the invention as claimed in the present application is clearly patentable over the combination of Walker and Schneier.

Regarding claim 16, first, it is noted that, in Walker, the measurement certification device is itself regarded as a trusted device: it is contained within a secure perimeter 70 to prevent tampering (column 7, lines 23-57). Thus, there would clearly be no reason for one skilled in the art to contemplate using a third-party arbitrator to certify the output from the device. Indeed, if the device were not trustworthy, having an arbitrator certify its output would be pointless.

Second, it should be noted that Schneier is exclusively concerned with electronic digital communications and in particular the passage referred to on page 35 is concerned with digital signing of electronic digital messages. There is no suggestion in Schneier that these digital techniques might be used for paper documents. The only reference Schneier makes to paper documents is to the conventional use of handwritten signatures on documents. Thus, it is submitted that Schneier clearly would not suggest to a person skilled in the art using a digital signature from a third part arbitrator to certify Walker's paper printout (column 10, lines 26-29).

Third, there is no suggestion in Walker of checking whether the measurement certification device is "authorized" to perform the test before printing out a measurement is printed. Moreover, Schneier is concerned with authentication rather than authorization: Schneier's digital signatures certify that a document originated from a particular person and has not been altered, but they do not check that the person was authorized to produce that document. Therefore, Schneier would

clearly not have suggested to a person skilled in the art the step of checking whether Walker's measurement device is *authorized* to perform the test.

Regarding claims 3 - 4 and new claims 17 - 19, although Walker suggests printing the certified measurement on a piece of paper (column 10, lines 26-29), it is respectfully submitted that there is no absolutely no suggestion that this piece of paper would have any information (such as a serial number) pre-printed on it (in bar code form or otherwise), and no suggestion of using such a pre-printed serial number in forming an authentication code. Walker (column 8, lines 22-34) mentions the use of a unique device identification number, but this is clearly not pre-printed on the piece of paper. Schneier clearly teaches nothing about pre-printing information, and is completely irrelevant to these claims.

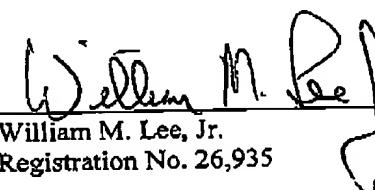
New claim 20 corresponds to original claim 5, rewritten in independent form including all the limitations of the base claim and intervening claims. As indicated in paragraph 19 of the detailed action, it is believed that claim is clearly allowable.

*Conclusion*

In summary, it is submitted that this application is now clearly in order for allowance and such action is respectfully solicited.

Respectfully submitted,

Date: August 9, 2004

  
\_\_\_\_\_  
William M. Lee, Jr.  
Registration No. 26,935

Barnes & Thornburg LLP  
PO Box 2786  
Chicago IL 60690-2786  
(312) 357-1313 Telephone  
(312) 759-5646 Facsimile  
(312) 214-4811 Direct